Securing the Core University Business Processes

Veliko Ivanov, Monika Tzaneva, Alexandra Murdjeva, Valentin Kisimov

Securing the Core University Business Processes

Veliko Ivanov[1], Monika Tzaneva[1], Alexandra Murdjeva[1],
Valentin Kisimov[1]

[1] University of National and World Economy, 8 December Str., Student Town, 1700 Sofia, Bulgaria

veltex@abv.bg, monika_tzaneva@yahoo.com, amurjeva@abv.bg, vkisimov@gmail.com

Abstract. In the paper are presented solutions for securing the core University Business Processes. A Method for identification which Business processes are critical for security point of view, on which is required to pay more attention for its securing. For securing of the elected Business processes is developed a new security system – Extended Certification Authority. Special Secure eDocument Management Architecture is developed, on which base are developed the solutions for securing the following University Business processes - Delegation of exam permissions to lecturers, Recording exam marks, and Exchange management documents.

Keywords: Securing business process, Extended Certification Authority, Secure eDucument Management Architecture.

1 Introduction

There are few definitions of the term “Business process”, which are not too different each other. In our research we have accepted the definition of [4], which under Business process understands a set of interrelated tasks leading to create a product or a service. Each Business process needs to have required security of its execution. This means the process should provide the security triangle of parameters Availability, Confidentiality, and Integrity, in an appropriate level.

University is like any other enterprise – with a set of business processes, from which some are more critical from security point of view. The criticality is coming from the generation of the university end result – the degree document, where all exam marks make its content. The processes leading to forming the university end result defines the set of core processes. Based on the mentioned criteria for the criticality, it is not too difficult to list the university core business processes.

The main goal of the current research is to identify what level of security the core business processes need, e.g. which the core university business processes needing higher level of security are, what is the needed security level, and how to provide that security.

2 Method for selection of core business processes needing high security

There is not standard way for selection of core business processes which need some level of security. There are some practical approaches - [5] and [6], which resolve particular private needs, but no one exists for university business processes security evaluation. For this reason we have developed our "Method for selection of core business processes needing high security".

The proposed Method works with number of University Business processes, which core set consists of 11 processes, identified in general, and more specifically for the case for our particular research – University of National and World Economy (UNWE), Sofia, Bulgaria. These 11 University Business Processes are:

- Delegation of exam permissions;
- Recoding exam marks;
- Exchange Academic Counsel (AC) reports;
- Exchange Rectors' Counsel (RC) reports;
- Exchange Faculty Board reports;
- Exchange Departmental Meeting reports;
- Review Public statements;
- Change the Educational Curriculums;
- Admittance of new students;
- Admittance students from 2nd to 3rd year;
- Change student status.

These business processes are evaluated from the needed security point of view via 9 criteria, grouped in 5 groups. The evaluation is provided with metrics 1 to 3, where 1 means needed low security requirement, 2 means medium and 3 means high. The following criteria are identified with the specified value and security impact:

a) Business Continuity – the criterion identifies what are the requirements for the Business continuity from the University business process;
b) Disaster Recovery – the criterion identifies the need for available recovery and the time for recovery of the University business process;
c) Event management – the criterion identifies how critical are the events for security violation for the business process;
d) Availability – the criterion identifies how critical is the business process to be available. Normally the availability is measured in percentage, but for the purpose of the current Method, these percentages are transformed into value 1 to 3 (from 0 to 33% - value 1, from 33% to 66% - value 2, and up to 99% - value 3);
e) Confidentiality – the criterion identifies how critical is to have encryption of the information for the business process and the level of encryption. This is an integrated criterion, where the percentage of the encrypted messages is evaluated, the type of encryption (symmetrical / asymmetrical), the key length, and the period of key refreshment;

f) Integrity – the criterion identifies the need of information integrity provided via security means;
g) Business impact – the criterion identifies what is the Business impact of the Business process to the entire University business security. This criteria is formed from a few sub-criteria:
    - Relative number of beneficiaries (students, professors, staff) impacted from the Business process;
    - Relative number of providers (external and internal) impacted from the Business process;
    - Level of cost of this Business process compared with the total cost of university processes;
    - Level of monthly transactions executed from the Business process;
    - Political sensibility of the Business process, which relates to the view of the University to the country and to the entire world, the effect of the Business process to the reputation of the University, the effect of the Business process to the high-education process in Bulgaria and Europe;
    - What is the overall impact to the University from the specific Business process;
    - What is the overall impact to professors (lecturers) and students from the specific Business process;

The collection of values from the above mentioned sub-criteria for Business impact is proposed to be done via a table – Table 1;

Table 1. Forming of Business Impact criteria

Business processes	Relative number of benefi-ciaries impacted	Relative number of providers impacted	Level of costs of this business process compared with total cost of university	Level of of monthly transac-tions	Political sensitivity	What's the overall impact on the University	What's the impact on professors	What's the impact on students	*Total average score*
BP #1									
BP #2									
etc.									

Each sub-criterion is also evaluated via the measures from 1 (low level) to 3 (high level). For each Business process a Total average score is created, which is rounded to the values 1, 2 and 3. This value is the defined value for Business Impact for the specific Business process.

h) Risk level – the criterion identifies the level of which the risk of the entire University business can raise, based on the current business process. The University Business strategy and University Security strategy define levels of risk (there are no many universities in the world which have developed Business strategy and Security strategy, like the big corporation. In the current case of UNWE, the research team has identified the appropriate risks, based on interviews with the university management);

i) Minimum acceptance level – the criterion identifies which is the minimum security level, which is needed for the specified Business process. This criteria is formed from a few sub-criteria:
   - Eligibility - inquires and responses of the Business process;
   - Enrollment and Disenrollment of data for/to the Business process;
   - Authorization – requests and responses to the Business process;
   - Claims – receipts and adjudications from the execution of the Business process;
   - Claims status - requests and responses from the execution of the Business process.

The collection of values from the above mentioned sub-criteria for Minimum acceptance level is proposed to be done via a table – Table 2;

Table 2. Forming of Minimum acceptance level criteria

Business process	Eligibility – inquiries & responses	Enrolments & Disenrollments	Authorization – requests & responses	Claims – receipts & adjudications	Claims Status – inquiries & responses	*Total average score*
BP #1						
BP #2						
etc.						

Each sub-criterion is also evaluated via the measures from 1 (low level) to 3 (high level). For each Business process a Total average score is created, which is rounded to the values 1, 2 and 3. This value is the defined value for Minimum acceptance level for the specific Business process.

The proposed Method for selection of business processes and their level of needed security uses a table, shown in Table 3 below.

Table 3. Business processes selection for needed security.

#	***Business process***	*Participating in:*			*Degrade level*			Bus. impact	Risk level	Min Accept. Level	Total score
		Bus. Cont.	Dis. Recov	Event Mgmt	Avai-labil.	Confi-dent.	Inte-grity				
1	**Delegation of exam permissions**	2	2	2	2	3	2	3	1	3	20
2	**Recoding exam marks**	3	3	2	3	3	3	3	2	3	25
3	**Exchange AC reports**	3	3	1	2	1	1	3	1	3	18
4	**Exchange RC reports**	3	2	1	2	1	1	3	1	3	17
5	Exchange Faculty Board reports	2	1	1	1	1	1	2	1	2	12
6	Exchange Departm.Meet. reports	2	1	1	1	1	1	1	1	1	10
7	**Review Public statements**	3	1	1	3	1	1	3	2	3	18
8	Change the Educ. Curriculums	1	1	1	1	1	1	1	1	1	9
9	**Admittance of new students**	3	3	2	3	1	1	3	2	2	20
10	**Admittance students 2nd to 3rg year**	3	2	2	3	1	1	2	1	1	16
11	Change student status	2	2	1	2	2	3	1	1	1	15

For the target object – UNWE, particular values are resulted into the table. From those results we have concluded, that the core university business processes from security point of view are:

- **Delegation of exam permissions (Protocols) to lecturers;**
- **Recording exam marks; and**
- **Exchange management documents**
  - Exchange AC reports;
  - Exchange RC reports;

The Business process "Admittance of new students" has also relatively high score – 20, but because it is with relatively small infrastructure part of the University IS infrastructure, we will exclude it from our research activities. The Business processes Exchange Academic Counsel (AC) reports and Exchange Rectors' Counsel (RC) reports we can combine for the future presentation of research results, because their security requirements are closed. In this way we receive an aggregated business process called "Exchange management documents". For this reason, the mentioned 3 core business processes will continue to be the focus of the further research, presented in the paper.

3 Extended Certification Authority

For securing the core university business process is required a special solution with involvement of Certification Authority (CA) and Public Key Infrastructure (PKI). The required functions for securing the core business processes are logically between the functions of CA and functions of PKI.

Certification Authority generally is either independent system or it is an agent of a PKI. The user can do the main certification functions through its keys and certificate – authentication, encryption, digital signature, data integrity, non-repudiation, etc., while the certificate can be used also for reputable identification, timeframe for validity and specification of possible security functions. The security credentials are linked to the CA via the digital signature of the certificate, where the Public key is included, and the Public key recognizes the pair connection with its Private key. CA is an entity that issues security keys – Private and Public and Digital Certificates for use by other parties. The functions of the CA can be summarized into:

- Has its own Root certificate;
- Verify the identity of entities asking to issue certificate;
- Generate Private and Public keys;
- Issue digital certificate attesting to the identity;
- Digitally sign the certificate via its Root certificate;
- Store certificate and keys in the secure tokens;
- Play a role for the trust party;
- Maintain Certification revocation (CR) process, CR List and Repository
- Use OCSP protocol (On-line Certificate Status Protocol) for access to CR List

From other side, the PKI is set of hardware, software, policies and procedures needed to issue and maintain Asymmetrical and Symmetrical keys and Public Key Certificates incorporating different user's identities, and also to order, issue, register, store, distribute, renew, revoke and manage Public Key Certificates. PKI serves as a trusted third party between many end-users. The functions of the PKI are much bigger and complex than the CA, and they can be summarized into:

- Operate with CA, Registration Authority (to verify and accept requests for certificates) and Repository (repository for certificates and CR List);
- Provide Backup and Recovery for the purpose to restore lost or damaged Certificates;
- Update Key History – at any certificate change, to update the history logs (because of expiration or a name change). Any data secured using the older keys would not be accessible unless the older keys are kept in an archive;
- Revoke Certificates, when the Certificate is no anymore valid or it is discredited;
- Automatic Key Renewing and Certificate renewing – after the expire of the certificate, new Private key and Public key has to be issued, on which base a new Certificate has to be issued for the same user, with a process of automatic renewal of them to the end-used repository – smart cards or USB devices. Automated key recertification can update the certificate with a new expiration date when necessary, without manual intervention;
- Cross Certification – used to establish a trusted relationship between separate PKI's. This allows for a distributed and decentralized infrastructure;
- Support for Non-Repudiation – prevents a certificate owner from denying that data was sent using the owner's certificate;
- Time stamping – certifies that the time stamp on the secured data is set and it is accurate and valid;
- Client API – A means for an application to use the services offered by a PKI.

PKI is an expensive and difficult to operate system. Only limited number of companies has the luxury to own a PKI. University generally does not operate with budgets of the big companies, for which reason it is not practical to expect that a University will create or buy a PKI. The world has established and easier approach to the PKI, defining "Small PKI". Small PKI was born out of a joint effort to overcome the over complication and scalability problems of traditional PKI, decreasing the role of RA, Repository, and some of the functions. The functions of the Small PKI cover all functions of the CA, with incorporation of some functions of the PKI. In summary, the functions of Small PKI can be listed as:

- Full CA functions;
- Mechanisms to support security in a wide range of Internet applications, including IPSec protocol;
- Keys renewal and key management;
- Encrypt electronic mail and WWW documents;
- Range of Secure application functions requiring use of Public key Certificates as ePayment and B2B;

- Support a range of trust models.

The analysis of the security needs for securing the core university business processes shows that the functionality of the Small PKI is too rich from security point of view and a university does not need of such a system. Here we have to add that the Small PKI is also an expensive system for the university budget and to securing the core University Business Processes we need a system, which functions are between those of CA and Small PKI. We call such a system "Extended CA" and position it in the functional axe of crypto functionality in a way, shown in figure 1.

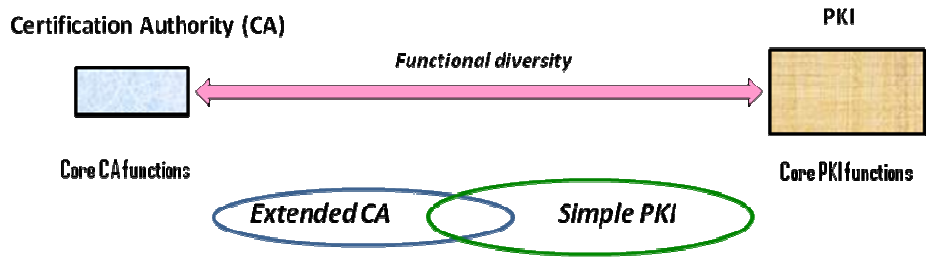

Fig.1. An axe of crypto functional systems, where the place of "Extended CA" is defined to be between CA and Small PKI

The authors have analyzed the functions needed for securing the core university business processes, providing cost-functions analysis. On this base a crypto system with the name "Extended CA" was designed, which is relatively cheap from university budget point of view and functionally reach for security point of view. We have found that the Extended CA has to be a CA with LDAP, Web server for communications, and supporting some PKI services such as digital signature, keys exchange, email encryption, and secure token support. After that analysis, we have concluded that the Extended CA has to have the following functions:

- To function of Full Certificate Authority (CA) and support of Certificate Revocation Lists (CRL);
- To operate with Directory server for storing security credentials;
- To use Web server for users' communication, exchange of information and auditing of all security transactions and operations;
- To provide Kerberos authentication;
- To use tokens (Smart cards and/or USB devices with smart cards) to store the security credentials inside;
- To support Securing web servers;
- To support Securing email;
- To provide Digital signature in off-line and on-line modes;
- To execute Application signatures (i.e. Signed drivers or ActiveX controls);
- To support Encrypted File Systems (EFS) and work with appropriate recovery agents;
- To support Smart Card Logins.

There are two standards (RFC) for certificates – for Public Key Certificates [7] and for Attribute Certificates [8]. The most used certificates in the world are the Public Key Certificates. At the same time, the Attribute Certificates provides some futures, which can be used for securing in a good way the university business processes. Generally, attributes in Attribute Certificate offer user's short-lived information and dedication, such as user's roles and access permissions, which suite the university short term access permissions, like giving access of a professor to exam marks for a subject, valid for a block or semester. For this reason the capabilities of the attributes in Attribute Certificate is preferably to use for the university purposes. For this reason we have analyzed the suitability of incorporation both certificates values into a single certificate, covering the international standards. We went to a conclusion, that the Extended CA can provide certificates, which combine the usability of both certificates.

Our proposed solution for a Certificate, issued by the Extended CA is to include the necessary attributes, which normally are part of the Attribute Certificate, in the Private Extensions of the Public Key Certificate. Applying the proposed approach, the certification issued by the Extended CA will have the following value-added functionality:

- Secure identification and authentication using pure SSL protocol + LDAP server;
- Separation access control based on SSL managed certificates;
- Add complementary security credentials, e.g. second PW, Biometric identification, etc.;
- Easy to manage Private information in Corporate (in our case – University) systems;
- Public Key Certificate (PKC) is per user, the attributes are “per group”, and integration of both is for relatively medium-term certificate, e.g. per semester;
- Provide “Revocation” for attributes;
- Security policy defined per medium-term (per semester);
- Provide trust from different CA/PKI via incorporated additional PKC (another way for cross certification);
- Incorporate Privilege attributes as Copy rights, Patents, Trademarks, access to management documents (levels and specific);
- Internet and Intranet specific rights;
- Role based control using attributes.

4 Secure eDocument Management Architecture

The elected core University Business Processes for security operate predominantly with electronic documents. Like in any corporate Information System, solutions for a few problems can be a single integrated architectural solution. For this reason we have developed a special Security architecture, which will be the base for the securing the elected core University Business Processes. The developed architecture we called

"Secure eDocument Management Architecture". The purpose of the offered in the paper architecture is to manage in a secure different management documents, providing for them the necessary security features, which do not exist in general electronic documents. The Secure eDocument Management Architecture has two focuses of security features:

a) Securing the elements of the electronic document (eDocument);
b) Securing the transactions with the eDocuments.

The Secure eDocument Management architecture operates with Lecturer's PC, where the Secured document is processed, and with Web server, where the University Business processes have centralized for treatment. As part of the Web site is the explained above Extended Certification Authority. The Secured document operates with 3 security features:

- Marcos, activated on loading the document;
- eButton with integrated macros, activated on pressing the Button;
- Security fields, keeping encrypted information, which is decrypted on Lecturer's PC.

Graphically, the Secure eDocument Management Architecture can be presented in figure 2.

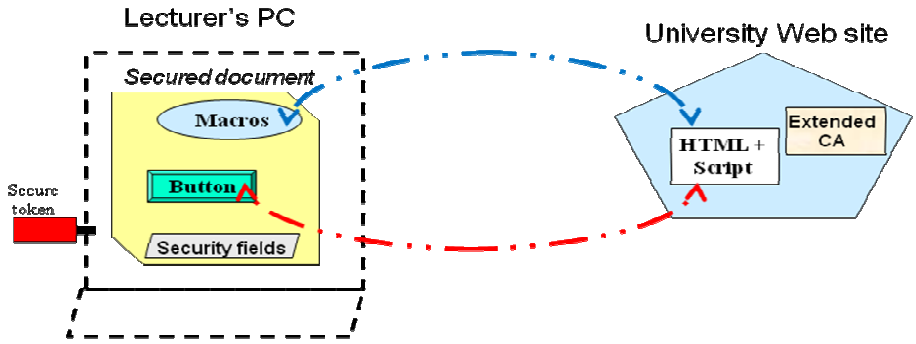

Fig.2. Conceptual architecture of Secure eDocument Management Architecture

The mentioned 3 security features are part of the eDocument. Having at least one of those security features, the eDocument is converted to a Secure eDocument. Each one of those 3 security features can exist in many instances in the Secure eDocument. The first security feature - Macros are programs, which are executed during the transaction (transferring) of the eDocuments from the Web site to the Lecturer's PC. For example, when a document is loaded from the University Web site to a Lecturer's PC, one of a few Macros can be executed automatically. The second security feature - Buttons are also programs, but activated by the user of the eDocument. For example, when a lecturer wants to digitally sign a document, he has to press a button, which keeps virtually a program code executing the process of digital signature. The third security feature – Security fields are part of the eDocument, which can be treated with different security algorithms, for example the field can be encrypted and only with the

wish of the end-user (lecturer) the field would be decrypted and represented in a plain text (via pressing of a button or executing of a Macros).

The developed Secure eDocument Management Architecture is used in securing of the presented below 3 core University Business processes.

5 *Secure Process*: Delegation of exam permissions to lecturers

The exam permission is a university document called Protocol, which specify which students to which subject have rights to be examined, by which lecturer. Not all student studying appropriate subject have rights to be examined at the end of given semester – they are different university procedures permitting under which conditions a student can go to be examined, for example if he finalized all assignments during the semester.

The current process can be secured using the explained in the previous section Secure eDocument Management architecture. We have designed, the Macros embedded in the eDocument – Protocol to provide the following functions:

- Full document protection via Password (via the lecturer's ID);
- Partial Confidentiality – some fields are only readable by the specified lecturer - Protocol name, Protocol number, semester validity;
- Document data integrity – Protocol checking on receiving;
- Checking the document time period validity: Document data creation – Document date receiving;
- Document digital signature verification.

The Macros also provide 3 additional security functions, related to the entire eDocument:

- Protocol cannot be read and used by non-dedicated lecturer;
- Protocol cannot be operated by non-dedicated lecturer;
- Lecturer cannot take a Protocol, which is not created by the University Information Security system.

The eDocument-Protocol is developed with 2 buttons:

- Accepting the document after visual control;
- Non-repudiation of receiving the eDocument.

6 *Secure Process*: Recording exam marks

The process of Recording the exam marks is associated with moving the exam marks from the eDocument-Protocol to the Information system "Student", where all exam marks are recording. Based on those exam marks are generated the degree documents. The manual process is related to many paper records, and using many clerks. At the end, the responsibility for the exam results is to the lecturer, but many other people

participate between the lecturer and the computer record of the exam marks. To eliminate all those interim people who do not keep responsibilities, is developed the current security process.

The securing of that business process uses a few security features:

- Secure eDocument-Protocol;
- Digital signing of the Protocol by the lecturer, before entering it into the system "Student";
- Using of One Time Password (OTP) for additional authentication of the lecturer;

The sequence diagram of the securing of the specified University business process is presented in figure 3.

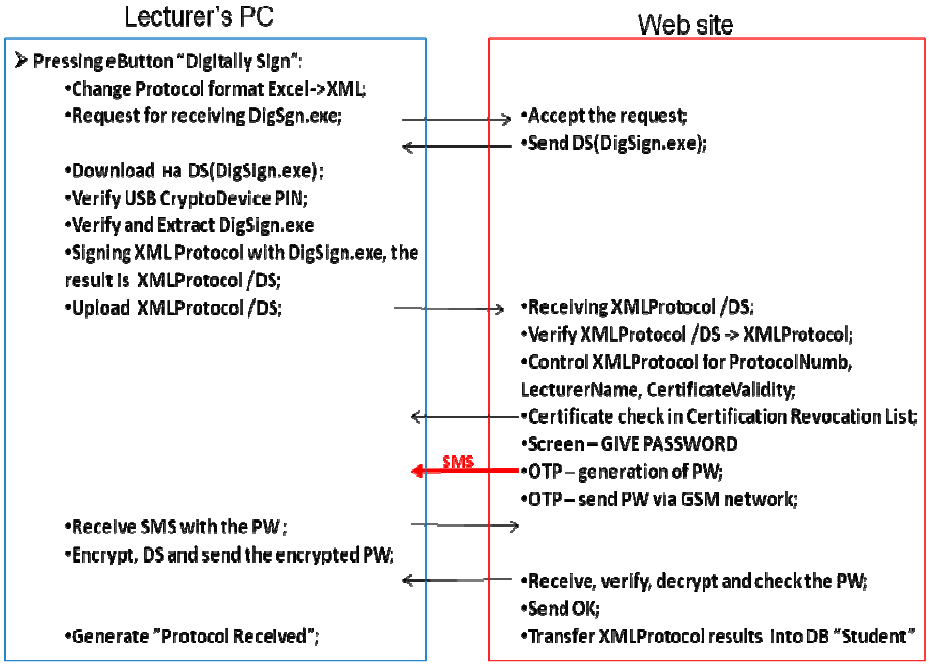

Fig.3. Control flow of the secure technologies used to secure the Business process "Recording the exam marks"

There are few special security technologies used in that diagram:

a) The program for Digital signing of the eDocument-Protocol is always loaded from the University Web site, just before the signing. This ensure correct digital signing;
b) The lecturer uses an USB Crypto device, which stores the Private key and the Certificate of the lecturer. To access those security credentials, the lecturer should enter the PIN code of the USB Crypto device;

c) During the signature verification, the major elements of the lecturer's certificate are checked, like whether that lecturer has right to enter the Protocol in the system "Student", what are the credibility of the lecturer in its certificate according to the subject for which the exams are entering, etc.;
d) The complex signature verification includes also the check whether the certificate is part of the Certification Revocation List (CRL). In the proposed solution CRL is not web accessible, but via an internal interface, because the check is provided inside the University Web site, where the Extended CA is also part of;
e) The OTP has a special solution which ignores its major security weakness – man-in-the-middle. This solution implement encryption and digitally signing the received password by the lecturer and then send it to the Web site. These both technologies identify and authenticate exactly the lecturer and the University Web site, working with entering the exam marks.

7 *Secure Process*: Exchange management documents

The Business process of Exchange management documents is designed as Peer-to-peer exchange of encrypted documents. This peer-to-peer link is a logical link, using the University Web site as an interim and control station. The main message moving mechanism used in the proposed solution is the emailing. The idea is to use exactly two interim stations – Web site and email server. The Web site is part of the Secure eDocument Management Architecture, which use as subsequent messaging mechanism for emailing. The conceptual architecture of that security architecture is presented in figure 4.

It is important to mention that the email services which are involved in the solution can be a corporate Email server or a Cloud Computing email services.

The developed solution provides as additional security features:

- Detail logging of all transactions – in the Web server;
- Auditing of all transactions – also in the Web server;

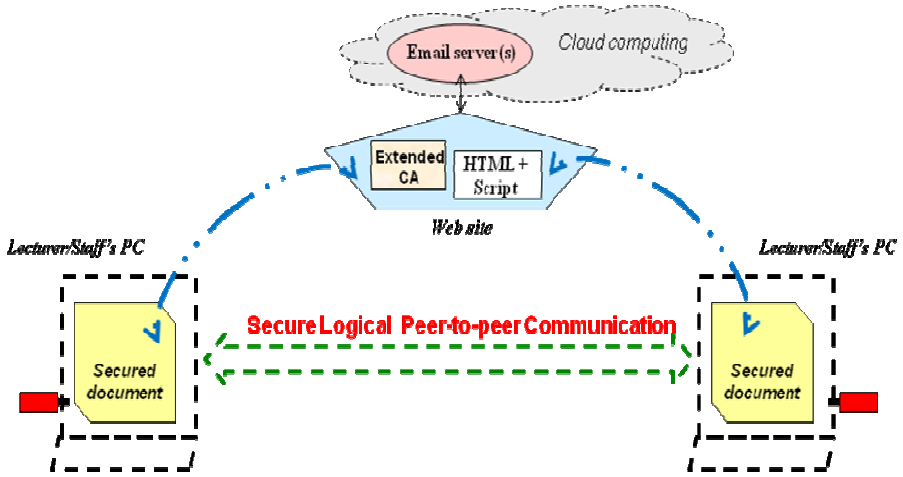

Fig.4. Architecture for secure exchange of management documents

9 Conclusions

The presented security solutions for securing of the core University Business Processes are based on electronic document incorporating security program code in a few ways, integrating existing security technologies, but executed in a secure ways, using new security system – Extended Certification authority. The prototyping of the proposed solution uses documents based on MS Office, while the security technologies for them have been developed in two platforms – Java and VB-.Net. Both platforms showed equal flexibility for operation and security quality. The proposed research has few open research problems, like a Framework for development of Extended Certification Authority, and well securing the University Web site (with integration with Extended CA), if it is not in the University Intranet, but on open Internet.

References

1. Brian O'Higgins, What is the Difference Between a Public-Key Infrastructure and a Certification Authority?, http://www.opengroup.org/comm/the_message/magazine/mmv4n2/pki.htm
2. M.Shirbu, J.Chuang, Distributed Authentication in Kerberos using Public key cryptography, http://people.ischool.berkeley.edu/~chuang/pubs/pkda.pdf
3. Bass de Graeff, Business processes Security, Unisys, http://www.unisys.com/unisys/ri/wp/detail.jsp?id=17600051

4. V.Kisimov, Dynamic Business-managed Information systems, Sofia, Bulgaria, 2008, ISBN 978-954-323-444-8 (2008)
5. R.Garfamy, Supplier selection and Business process improvement, doctoral thesis, Autonomous University of Barcelona, (2005)
6. J.Lee, J. Choi, Process selection for Business Process Management in a mobile telecommunications company, University of Illinois at Urbana-Champaign, USA, International Journal of Information Technologies and Management, Vo8, No4, pp. 382-399, (2009)
7. RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt
8. National RFC 3281, An Internet Attribute Certificate Profile for Authorization, http://www.faqs.org/rfcs/rfc3281.html